REMARKS

Claims 1-13 are pending in the present application. The Office Action and cited references have been considered. Favorable reconsideration is respectfully requested.

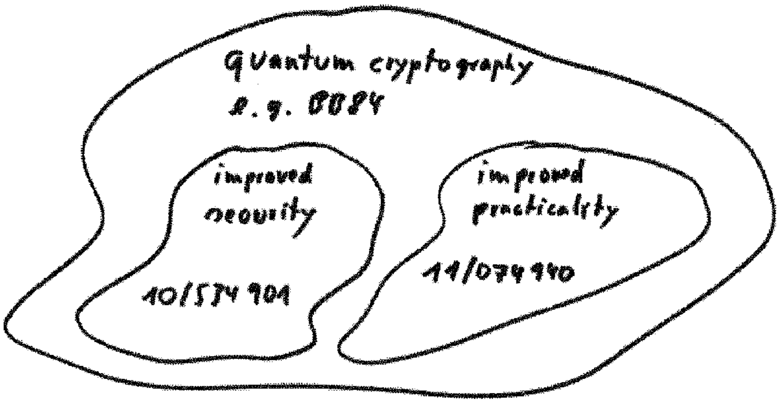
Claim 1 is rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 1 has been amended to remove the word "the" from before "quantum states", thus correcting the antecedent basis informality. Withdrawal of this rejection is respectfully requested.

Claims 1 and 6-7 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claim 1 of copending Application No. 11/074,940. This rejection is respectfully traversed for the following reasons.

Claim 1 recites a method for exchanging a secure cryptographic key for a quantum cryptography apparatus employing non-ideal elementary quantum systems, wherein the apparatus comprises an emitter and a receiver, being connected by a quantum channel and a conventional communication channel, the emitter encodes each bit at random onto a pair of non-orthogonal states belonging to at least two suitable sets, there is not a single quantum operation reducing the overlap of quantum states of all sets simultaneously, the emitter sends the encoded bit along the quantum channel to the receiver, the receiver randomly chooses an analysis measurement within said suitable sets, the emitter sends a set information along the conventional communication channel, the receiver discards all received encoded bits for which it has chosen a different analysis measurement incompatible with the set they belonged to and sends an appropriate information to the emitter along the conventional communication channel. This is not taught, disclosed, or made obvious by the prior art of record.

Applicant thanks the examiner for his indication that the subject matter itself is considered allowable, if the provisional double patenting rejection issue is solved.

Furthermore, Applicant appreciates the inclusion of the table in the office action showing the subject matter in question. However, Applicant respectfully submits that the subject matter of the claims of the two applications are directed to different issues. Patent applications 10/534901 (the '901 application) and 11/074940 (the '940 application) are both in the field of quantum cryptography, but they do cover different inventions in spite of their apparent similarity. Applicant will show that one application comprises features directed to improve security of the quantum cryptography method and the other application comprises features directed to improve practicality of the quantum cryptography method. The principles of quantum cryptography are the link which is noted in the encompassing structure to show the starting point of the discussion:



Before explaining how these inventions differ, it is useful to describe the basic principles of quantum cryptography as introduced by Bennett and Brassard in 1984 (also known as the BB84 protocol):

An emitter and a receiver want to communicate a secret sequence over a channel in such a way that an interception can be detected. If they used a conventional communication channel, i.e., a channel using objects described by classical physics to carry the bit values, they would not be able to detect such an interception. Instead they resort to using a quantum channel, where bit values are coded on quantum objects (note that in the claims of the above mentioned applications, the term "quantum systems" is used instead of "quantum objects"), such as photons or weak laser pulses with the bit values coded on its polarization state. Two sets of two polarization states are used. The first set consists of the vertical and horizontal polarization states, where, for example, vertical codes for a "1" bit value and horizontal codes for a "0". The second set can consist of the diagonal polarization states, with a similar bit value coding convention (e.g. "1" is +45° and "0" is -45°).

Every time the emitter wants to send a bit value, he selects randomly which set of states - horizontal/vertical or diagonal - will be used to code it. If, for example, he wants to send a "1", he can choose between the vertical state or the +45° state).

The receiver has two analyzers to measure the state of the incoming photons: one - the horizontal/vertical analyzer - allows to distinguish between photons with horizontal and vertical states and the other one - the diagonal analyzer - allows to distinguish between photons with +45° and -45° diagonal states.

Every time the receiver receives a photon from the emitter, he randomly selects which analyzer he uses.

When the analyzer of the receiver is compatible with the set of states in which the emitter has prepared the photon, the result the receiver obtains is identical to the bit value sent by the emitter. When the analyzer is not compatible, the value measured by the receiver is not correlated with that sent by the emitter.

After transmission of the photon, the emitter tells the receiver which set the photon belonged to, so that the receiver can check whether he selected the right analyzer and whether the bit should be kept or discarded.

An eavesdropper intercepting the photons would necessarily introduce errors in the sequence, as he would sometimes select the wrong analyzer. These errors will reveal his action.

Although the BB84 system would be just fine a perfect world, there are practical limitations for such a method. The inventions of the '901 and '940 application aim at improving such basic quantum cryptography devices, but they do so in different ways.

The '901 application aims at improving the security of quantum cryptography when non-ideal quantum states are used. BB84 called for the use of ideal quantum objects in the form of single-photons (one and only one photon for each bit). Producing such quantum objects is however very difficult in practice and most demonstrations have relied on weak laser pulses. Unfortunately, such pulses sometime contain more than one photon, which opens a security loophole in the BB84 protocol. In the '901 application, the inventors propose to change the way the states of the quantum objects are selected and the sets of states are formed to reinforce the protocol. The central idea is to add the condition that "there is not a single quantum operation reducing the overlap of the quantum states of all sets simultaneously" (Claims 1, 6-7). It is important to note that in the BB84 proposal with non-ideal quantum systems, it is possible to find a single quantum operation reducing the overlap of the quantum states of all sets simultaneously. This operation could be used by an eavesdropper to intercept the bit sequence without introducing errors, which defeats the purpose of quantum cryptography.

As for **the '940 application**, it aims at improving the practicality of a quantum cryptography system, whether it uses the BB84 protocol or another protocol. It was explained above that in the BB84 proposal, the emitter selects randomly for each bit of the sequence independently the set of quantum states are used to encode the bit value. This approach works, but is difficult to implement in practice. One random bit of information corresponding to the set of quantum states is required for each bit of the sequence. These random bits can be difficult to generate when the bit rate is high. They must also be stored by the emitter until they are compared with the receiver, which again is difficult when the bit rate is high. The same difficulties arise at the receiver's side. Moreover, changing the set of quantum states for each photon is not necessary for security. It is possible to achieve the same level of security by keeping the same set of quantum states for several photons, which constitutes the invention of the '940 application: "the emitter encodes blocks of N bits ... where the same encoding basis (i.e. the same set of quantum states) is used for all N bits within a given block" (Claim 1).

In conclusion, although the inventions presented in these two patent applications can be combined to improve the security ('901 application) and practicality ('940 application) of a quantum cryptography system, they are clearly independent and different. This can also be seen in the table as provided in the office action. In addition to the portions not printed in bold in the table, there are additional differences between the claims (especially in the copending application claim), showing that they are directed to functionally different teachings.

Within the method of the instant application 10/534901 the emitter encodes each bit at random (onto a pair of non-orthogonal states) wherein there is not a single quantum operation reducing the overlap of the quantum states of all sets simultaneously and the receiver accepts or discards encoded bits (with feedback along the conventional communication).

Copending application 11/074940 does not require said condition from the instant application (i.e., there is not a single quantum operation reducing the overlap of the quantum states of all sets simultaneously) as prerequisite for the method of the copending application to work. Instead there is a different requirement. The emitter chooses a block size N, wherein N>=2 and encodes blocks of these N bits (erroneously printed in bold in the table of the office action). At the same time the receiver chooses the analysis basis also for every block of N bits (erroneously printed in bold in the table of the office action) and informs the sender about the result of the measurement accordingly.

Therefore there is no functional equivalence between the two applications and the two claims are to be considered patentably distinct. It is clear in the light of the above explanation that the examined application claims are not anticipated or could be considered obvious over the reference claim(s).

For at least these reasons, Applicant respectfully submits that claims 1 and 6-7 are patentable over the copending '940 application.

In view of the above amendment and remarks, Applicant respectfully requests reconsideration withdrawal of the outstanding rejections of record. Applicant submits that the application is in condition for allowance and early notice to the effect is most earnestly solicited.

If the Examiner has any questions, he is invited to contact the undersigned at 202-628-5197.

Respectfully submitted,

BROWDY AND NEIMARK, P.L.L.C.
Attorneys for Applicant(s)

By /Ronni S. Jillions/
Ronni S. Jillions
Registration No. 31,979

RSJ:srd
Telephone No.: (202) 628-5197
Facsimile No.: (202) 737-3528
G:\BN\I\isle\Gisin1A\pto\2007-11-15Amendment.doc